Anonimato Incondicional en Sistemas de Voto Electrónico Presencial

Pablo García [1]; Silvia Bast [1]; Germán Montejano [1 2]

[1]Departamento de Matemática
Universidad Nacional de La Pampa
Av. Uruguay 151 – (6300) Santa Rosa – La Pampa – Argentina
Tel.: +54-2954-425166– Int. 28
[pablogarcia, silviabast]@exactas.unlpam.edu.ar

[2]Departamento de Informática
Universidad Nacional de San Luis
Ejército de los Andes 950 – (5700) San Luis – San Luis – Argentina
Tel.: +54-2652-424027 – Int. 251
gmonte@unsl.edu.ar – web: http://www.unsl.edu.ar

Resumen

La discusión sobre la viabilidad de la implementación del voto electrónico parece interminable. Por ejemplo, luego de arduas discusiones legislativas, el Congreso de la Nación ha rechazado la propuesta del Poder Ejecutivo Nacional de implementar un sistema de boleta única electrónica. En los últimos días, un importante grupo de expertos informáticos de Universidades Nacionales se manifestaron en contra del voto electrónico[1] e invitan a firmar una adhesión a tal rechazo[2].

En un momento de la historia en el que por medios digitales se hacen múltiples operaciones que involucran, por ejemplo, grandes cantidades de dinero o riesgo para vidas humanas, parece apresurado afirmar que es imposible generar un sistema de votación electrónica que resulte apropiado.

Si se analiza en detalle, la característica distintiva de este tipo de sistemas es la necesidad de mantener el anonimato de quienes emiten un sufragio. En otros aspectos, el voto electrónico no se diferencia demasiado de otras aplicaciones cuyo uso se encuentra absolutamente generalizado.

Este documento expone una serie de avances que, en el ámbito de un Proyecto de Investigación que involucra a los autores, se han obtenido en el tema de la privacidad del votante, que es el punto más complejo de resolver en un sistema de E – Voting.

Palabras clave: ***E-Voting, Anonimato Incondicional, Secreto Perfecto, One Time Pad, Recuperación de Colisiones, Voto Presencial.***

[1] http://www.cronista.com/economia politica/Expertos-universitarios-lanzaron-una-campana-contra-el-voto-electronico-20161101-0113.html

[2] http://www.dc.uba.ar/solicitada-voto-electronico

Contexto

Este trabajo se enmarca el Proyecto de Investigación: "Aspectos de Seguridad en Proyectos de Software", que se desarrolla en el ámbito de la Facultad de Ciencias Exactas y Naturales de la Universidad Nacional de La Pampa (UNLPam), Resolución N° 488/14 del Consejo Directivo. Tal proyecto surge desde la línea de Investigación "Ingeniería de Software y Defensa Cibernética", presentada en [1], y que a su vez se enmarca en el Proyecto "Ingeniería de Software: Aspectos de alta sensibilidad en el ejercicio de la Profesión del Ingeniero de Software" de la Facultad de Ciencias Fisíco - Matemáticas y Naturales de la Universidad Nacional de San Luis (UNSL) y que incluye acciones de cooperación con la Universidad Federal de Minas Geráis (UFMG, Brasil).

Entre tales acciones deben mencionarse:

- Pablo García realizó una estadía de un año en la Universidad Federal de Minas Geráis (UFMG), aprobando seminarios de posgrado y trabajando en el grupo "Criptografía Teórica y Aplicada", dirigido por Jeroen van de Graaf, PhD. Desde el 1/3/2012 hasta el 15/12/2012.
- Jeroen van de Graaf, PhD., Docente de UFMG, y el Dr. Germán Montejano (UNSL) fueron orientadores del Mg. Pablo García en el desarrollo de su tesis de para obtener el grado de Magister en Ingeniería de Software, defendida en 2013.
- Pablo García realizó una estadía de intercambio y actualización en el laboratorio 4303 de DCC, ICEX, UFMG, a través de una beca CAFPBA. Desde el 18/10/2106 hasta el 18/11/2106.
- Se prevé otra estadía de un mes en 2017 para intercambio de avances en- tre el grupo de investigación UNLPam – UNSL y el de DCC (UFMG).

1. Introducción

Una de las premisas fundamentales para este grupo de investigación se refiere a la necesidad de otorgar seguridad incondicional a la privacidad del votante. En efecto, muchos esquemas de voto electrónico, (aquellos que se basan en Mix Nets, [2]), han otorgado seguridad incondicional al proceso de votación (que sólo debe ser protegido por las diez horas que dura la elección) y seguridad computacional al anonimato, que debe asegurarse indefinidamente.

Bajo el convencimiento de que esa propuesta es incorrecta, se buscan alternativas que operen de manera exactamente inversa, asegurando el secreto eterno de la opción que realizó un votante, aún sabiendo que esa información podría permanecer indefinidamente disponible en medios digitales para su análisis.

Los avances en ese sentido fuero desarrollándose en múltiples publicaciones desde 2014 hasta la fecha (por ejemplo, [3] y [4]) y fue- ron finalmente recopilados y revisados para la publicación, como libro, en [5].

En consecuencia, se comenzó a trabajar en un esquema concreto e integral de voto electrónico presencial que atendiera a todas esas consideraciones y que, simultáneamente, otorgara niveles razonables de seguridad computacional a la hora de proteger el acto eleccionario. La primera versión de tal propuesta se denomina "OTP – Vote" y fue presentada en [6]

El esquema inicial, todavía en etapa de diseño final, propone dos condiciones básicas para garantizar la privacidad incondicional:

- Rigurosa separación de la identificación del votante y el acto de votación.
- Almacenamiento del sufragio en posiciones aleatorias (potencialmente diferentes) en un esquema basado en canales paralelos de slots.

Como consecuencia de lo anterior, las colisiones son posibles; por lo tanto, es factible perder votos. La implementación de canales paralelos de slots es una optimización del esquema conocido como Birthday Paradox ([7]), que enuncia lo siguiente:

"En un grupo de 23 personas, la probabilidad de que dos cumplan años el mismo día es superior a ½."

En la práctica, eso se relaciona con almacenar los sufragios en un único vector unidimensional. La alternativa propuesta implementa un conjunto de arreglos paralelos. Cada sufragio se almacenará una vez en cada canal, en posiciones aleatorias potencialmente distintas. Aplicando el nuevo esquema, un voto sólo se perderá si colisiona en todos los canales. La probabilidad de ese evento puede llevarse a cualquier valor exigido mediante la aplicación de las fórmulas presentadas en [8] y [9].

El esquema de múltiples claves, inspirado en [10], exige que para poder realizar un fraude, la totalidad de las personas que cuentan con una clave individual, deben ser corruptas. En efecto, con que uno sólo de los involucrados muestre una conducta honesta, cualquier intento de fraude será detectado.

Finalmente, OTP – Vote incorpora una técnica de recuperación de votos basada en XOR que disminuye aún más la probabilidad de pérdida de sufragios. De acuerdo con un alto número de simulaciones, la misma es despreciable si se administran apropiadamente los parámetros del sistema.

Concretamente, por la forma en que opera el modelo, no es posible que se pierda un único voto individual. Y la probabilidad de que se pierdan n votos (con $n > 1$), es que los mis- mos coincidan en todos los canales implementados. Los primeros análisis en ese sentido se presentan en [11] y muestran que, en las condiciones correctas, la probabilidad de que se pierdan sufragios puede minimizarse tanto como se desee.

2. Líneas de Investigación, Desarrollo e Innovación

OTP – Vote se encuentra en una etapa avanzada de su desarrollo. Si bien el esquema muestra características interesantes, quedan algunas cuestiones pendientes:

- Definir el sistema criptográfico exacto que se utilizará entre las estaciones de votación y los servidores.
- Formalizar los commitments necesarios para generar una comunicación confiable.
- Concretar, en base al punto anterior, un protocolo antifraudes que garantice una operación segura con un nivel aceptable de eficiencia.
- Desarrollar técnicas de Verificabilidad "End to End" que permitan, simultáneamente, la verificación individual de cada votante y la verificación global del resultado del proceso.

La concreción de los cuatro pasos mencionados permitiría construir un sistema de voto electrónico sólido y confiable.

3. Resultados y Objetivos

OTP – Vote es una propuesta para implementación de voto electrónico presencial que se obtiene como resultado de cinco años de investigación. En él se plasman todos los avances individuales que se fueron obteniendo desde 2012:

- Se implementa un sistema de almacenamiento basado en canales paralelos que minimiza de manera significativa la pérdida de sufragios por colisiones y garantiza el anonimato incondicional.
- Se utiliza una técnica basada en múltiples claves de estilo One Time Pad que garantizan secreto perfecto.
- Se aplica un modelo de recuperación de colisiones por XOR que refuerza la seguridad del modelo.

A futuro, se espera implementar todos los puntos mencionados (y los que aún están en análisis) en una aplicación concreta de voto electrónico.

4. Formación de Recursos Humanos

En el marco del presente proyecto se presentan múltiples acciones relacionados con la formación de recursos humanos:

1. Pablo García defendió su tesis para obtener el grado de Magister en Ingeniería de Software de la Universidad Nacional de San Luis, el día 13/11/2013. La tesis se tituló: "Optimización de un Esquema Dining Cryptographers Asíncrono" y fue dirigida por Jeroen van de Graaf, PhD (UFMG) y Dr. Germán Montejano (UNSL).
2. Silvia Bast defendió su tesis para obtener el grado de Magister en Ingeniería de Software de la Universidad Nacional de San Luis, bajo la dirección del Dr. Germán Montejano (UNSL) y del Mg Pablo García (UNLPam) el día 14/12/2016. La tesis se tituló: "Optimización de la Integridad de Datos en Sistemas de E- Voting".
3. Pablo García está desarrollando su tesis para obtener el grado de "Especialista en Ingeniería de Software". Su plan de trabajo fue aprobado y se planea su defensa para agosto de 2017. La tesis se titula: "Anonimato en sistemas de Voto Electrónico" y es dirigida por Jeroen van de Graaf, PhD (UFMG) y Dr. Germán Montejano (UNSL).
4. Silvia Bast está desarrollando su tesis para obtener el grado de "Especialista en Ingeniería de software". Su plan de trabajo fue aprobado y se planea su defensa para agosto de 2017. La tesis se titula: Sistemas de e-Voting: Integridad de Datos" y es dirigida por el Dr. Germán Montejano (UNSL) y del Mg Pablo García (UNLPam).
5. Estela Marisa Fritz: completó su etapa de capacitación en un tema en el que no era experta. Durante 2017 realizará todos los aportes relacionados con la temática de generadores aleatorios, insumo necesario para los nuevos avances en el proyecto. Los mismos deberían plasmarse en una te- sis de posgrado.
6. Silvia Bast y Pablo García completaron el cursado de la totalidad de los créditos para el Doctorado en Ingeniería Informática (FCFMyN – UNSL).

5. Referencias

[1] **Uzal R., van de Graaf, J., Montejano G., Riesco D., García P**.: "Inicio de la Línea de Investigación: Ingeniería de Software y Defensa Cibernética". Memorias del XV WICC. Ps. 769 - 773. ISBN: 9789872817961. 18-19/04/2013.

[2] **Jakobsson M., Juels a., Rivest R.:** "Making Mix Nets Robust for Electronic Voting by Randomized Partial Checking". USENIX Security '02, ps. 339-353. 2002.

[3] **van de Graaf J., Montejano G., García P.:** "Optimización de un Protocolo Non - Interactive Dining Cryptographers". Congreso Nacional de Ingeniería Informática / Sistemas de Información. CoNaIISI 2013. 21 y 22 de noviembre de 2013. Córdoba, Argentina
.

[4] **van de Graaf J., Montejano G., García P., Bast S**.: "Anonimato en Sistemas de Voto Electrónico". Memorias del XVI Workshop de Investigadores en Ciencias de la Computación 2014 (WICC 2014). Ps. 822 – 826. ISBN: 9789503410844.

[5] **García, P:** "Una Optimización para el Protocolo Non - Interactive Dining Cryptographers: una Propuesta Alternativa para Obtener una Implementación Eficiente". ISBN - 13: 978-3-639-85270-7. ISBN - 10: 3639852702. EAN: 9783639852707. Idioma: Español. Editorial Académica Española Número de páginas: 180. Fecha de publicación: 31/01/2017.

[6] **Bast S.:** "Optimización de la Integridad de Datos en Sistemas de E-Voting". Tesis de Maestría defendida en la Universidad Nacional de San Luis. 14 de Diciembre de 2016. San Luis, Argentina.

[7] **Flajolet P., Gardy D., Thimonier L.:** "Birthday Paradox, Coupon Collectors, Caching Algorithms and Self - Organizing Search". Discrete Applied Mathematics 39, ps. 207-223. North-Holland. 1992

[8] **van de Graaf J., Montejano G., García P.**: "Manejo de Colisiones en un Protocolo Non - Interactive Dining Cryptographers". Anales de las 42° Jornadas Argentinas de Informática e Investigación Operativa (JAIIO, ISSN: 1850-2776). Workshop de Seguridad Informática (WSegI 2013, ISSN: 2313-9110). Páginas 29 a 43. Septiembre 2013.

[9] **García P., van de Graaf J., Montejano G., Bast S., Testa O.:** "Implementación de Canales Paralelos en un Protocolo Non - Interactive Dining Cryptographers". 43° Jornadas Argentinas de Informática e Investigación Operativa (JAIIO 2014), Workshop de Seguridad Informática (WSegI 2014).

[10] **Broadbent A., Tapp A.**: "Information - Theoretic Security without an Honest Majority". Computing Research Repository - CORR. vol. abs/0706.2, ps.410-426, 2007.

[11] **García P., Bast S., Montejano G., Fritz E.:** "Codificación de Sufragios con Detección de Colisiones en NIDC con Canales Paralelos de Slots". Congreso Nacional de Ingeniería en Informática / Sistemas de Información. CoNaIISI 2016.